

CLAIMS

What is claimed is:

- 1 1. A digital signature method, comprising:
2 converting, on a computer system, digital data representative of a document
3 into a predetermined format;
4 applying the predetermined format and a viewer program to a hash function
5 to mathematically operate on the predetermined format and the viewer program
6 and provide a message digest, the viewer program for viewing the predetermined
7 format that is a representation of the document; and
8 encrypting the message digest using a private key to provide a digital
9 signature.
- 1 2. The digital signature method of claim 1, further comprising
2 incorporating into the digital signature a file including one or more parameters
3 specifying an environment of the computer system at the time of creation of the
4 digital signature.
- 1 3. The digital signature method of claim 2, wherein said one or more
2 parameters includes one or both of a type and version of one or more of the
3 following: a video card, monitor, operating system, application program, and
4 signing interface library of the computer system.

1 4. The digital signature method of claim 1 further comprising
2 timestamping the digital signature using a trusted source.

1 5. The digital signature method of claim 1 further comprising notarizing
2 the digital signature.

1 6. The digital signature method of claim 1, wherein the predetermined
2 format is a bitmap representation.

1 7. The digital signature method of claim 1 further comprising:
2 transmitting the digital signature, predetermined format, and viewer
3 program over a network to a receiver computer system;
4 decrypting the digital signature using a public key corresponding to the
5 private key, to recover the message digest;
6 applying the predetermined format and the viewer program to a hash
7 function, to mathematically operate on the predetermined format and the viewer
8 program to provide a calculated message digest;
9 comparing the calculated message digest with the recovered message digest;
10 if the calculated message digest is identical to the recovered message digest,
11 providing the predetermined format using the viewer program.

0050707" 88228960

3 monitor, operating system, application program, and signing interface library of the
4 first computer system.

1 17. The system of claim 11 further comprising a timestamp server coupled
2 to the network, said timestamp server to receive over the network, digitally
3 timestamp, and transmit over the network the predetermined format, viewer
4 module, and digital signature.

1 18. A method, comprising:
2 converting, on a computer system, a document into a predetermined format;
3 appending the predetermined format with a viewer program to provide a file
4 archive, the viewer program for viewing the predetermined format that is a
5 representation of the document;
6 applying the file archive to a hash function to mathematically operate on the
7 file archive and provide a message digest; and
8 encrypting the message digest using a private key to provide a digital
9 signature.

1 19. The method of claim 18, wherein the predetermined format is a bitmap
2 representation.

1 20. The method of claim 18 further comprising:

2 transmitting the digital signature and the file archive over a network to a
3 receiver computer system;
4 decrypting the digital signature using a public key corresponding to the
5 private key, to recover the message digest;
6 applying the file archive to a hash function, to mathematically operate on the
7 file archive to provide a calculated message digest;
8 comparing the calculated message digest with the recovered message digest;
9 if the calculated message digest is identical to the recovered message digest,
10 providing the predetermined format using the viewer program.

1 21. The method of claim 20, wherein providing the predetermined format
2 using the viewer program comprises one or more of the following:
3 viewing the predetermined format on a monitor using the viewer program;
4 printing the predetermined format using the viewer program; and
5 faxing the predetermined format using the viewer program.

1 22. The method of claim 18, wherein the viewer program is an executable
2 program.

1 23. A computer readable medium having stored therein instructions for
2 causing a central processing unit to execute the method of claim 18.

1 24. A digital signature method, comprising:

09687288-101300

